IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 5313
Xin Wang	)	Group Art Unit: 2135
Serial No. 09/469,726	)	Examiner: Ha, Leynna A.
Filed: December 21, 1999	)	
For: SYSTEM AND METHOD FOR	)	Date: April 30, 2007
DOCUMENT DISTRIBUTION	)	

REQUEST FOR RECONSIDERATION

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed October 31, 2006, Applicants respectfully request reconsideration and allowance of the application in view of the following remarks. Claims 1-22 are pending in this application, of which claims 1 and 13 are independent.

Claims 1-8, 10-20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,084,969 to Wright et al. and U.S. 6,587,946 to Jakobsson. However, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1-8, 10-20, and 22.

For example, independent claim 1 recites, in relevant part, a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document; encrypting the original document with the session key to create an encrypted document; *generating a proxy key based on a public key corresponding to the selected recipient*; and applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

In addition, independent claim 13 recites, in relevant part, a system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising a session key generation system that generates a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document; an encryption system that encrypts the original document with the session key to create an encrypted document; a proxy key generation system that *generates a proxy key based on a public key corresponding to the selected recipient*; and a transformation system that applies the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

Thus, claim 1 recites "generating a proxy key based on a public key corresponding to the selected recipient" and claim 13 recites "a proxy key generation system that generates a proxy key based on a public key corresponding to the selected recipient." According to the present invention, a proxy key is a key that is used to transform a message encrypted for one recipient into a message encrypted for another recipient without decrypting the message in the process. The Examiner's attention is respectfully directed to page 23, lines 18-23, of the Specification which provides that a proxy encryption scheme is public if the "proxy keys it generates may be published without compromising its security and proxy transformations applied in untrusted environments; otherwise, the scheme is private. In a private scheme, when a proxy key is transferred from the grantor to the facilitator and grantee, care must be taken to protect the proxy key from disclosure. As a result, the proxy transformation which uses the proxy key must be performed in private as well." (Page 23, lines 18-23). At least these features are not disclosed, suggested, or rendered obvious by the teachings of Wright or Jakobsson, alone or in combination.

Instead, Wright merely discloses a way of using a proxy (server) to decrypt and re-encrypt a message. In particular, the Examiner asserts that Col. 10, lines 26-28, and Col. 11, lines 11 and 65-67, and col. 14, lines 35-36, of Wright disclose "generating a proxy key based on a public key corresponding to the selected recipient." Applicants respectfully submit that this is not correct.

In particular, Col. 10, lines 26-28, reads as follows: "The user identification number (UID) . . . is used to indicate the source of the message so as to enable the pager proxy to retrieve the appropriate public decryption key (pb.sender)." This portion of Wright refers to the sender's key not to "a public key corresponding to the selected recipient." Moreover, there is no reference whatsoever to generating a proxy key.

Col. 11, line 11, reads as follows: "information stored in memory, including private and public key of the pager." The public key of the pager, i.e. the recipient, is mentioned, but there is no discussion of generating a proxy key based thereupon.

Col. 11, lines 65-67, read: "Turning to FIG. 4, the pager proxy 7 includes a database of public keys corresponding to the unique public keys of pagers registered with the encryption service provider that operates the proxy server." Once again, the public key of the pager, i.e. the recipient, is mentioned, but there is no discussion of generating a proxy key based thereupon.

Finally, Col. 14, lines 35-36, read: ".. field 2 of the packet is decrypted by the private key of the destination pager (step 410) and then by the public decryption key of the pager proxy server (step 420) based on the encryption method identified by the identifier in field 1." This quote refers to two decryption steps using the private key of the pager and the public decryption key of the server. It does not refer to the generation of a proxy key based upon the public key of the pager/recipient.

Thus, Wright fails to disclose, suggest, or render obvious the generation of a proxy key based upon the public key of the recipient. Moreover, even if the step of generating a proxy key is set aside, as an example, use of the pager's public key as a "proxy key" would result in a non-functional system wherein any recipient could convert encrypted messages for others into encrypted messages for themselves thereby rendering such a system completely non-secure. That is why a separate proxy key needs to be generated based upon the public key of the recipient.

Similarly, contrary to the Examiner's assertions otherwise, Jakobsson also fails to disclose or suggest the generation of a proxy key based upon the public key of the recipient. Instead, Jakobsson disclosed the use of the sender's private key (split into a number of shares) by quorum of proxy servers to perform the proxy transformation. It does not, however, use the recipient's public key to generate a proxy key.

For at least the reasons stated above, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious, the invention recited in independent claims 1 and 13 under 35 U.S.C. § 103(a). Dependent claims 2-8, 10-12, 14-20, and 22 are also allowable by virtue of their respective dependencies on claims 1 and 13, and also on their own merits. Therefore, Applicants respectfully request that the rejection of claims 1-8, 10-20, and 22 under 35 U.S.C. § 103(a) in view of Wright and Jakobsson be reconsidered and withdrawn.

Claims 9 and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and the article entitled Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition). However, none of Wright, Jakobsson, or the Irish Times article, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 9 and 21.

As is clearly presented above, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious the invention recited in independent claims 1 and 13. In this regard, the Irish Times article also fails to overcome the deficiencies of Wright and Jakobsson with respect to claims 1 and 13.

Thus, for at least the reasons stated above, none of Wright, Jakobsson, or the Irish Times article, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1 and 13 under 35 U.S.C. § 103(a). Rejected dependent claims 9 and 21 are also allowable by virtue of their respective dependencies on claims 1 and 13, and also on their own merits. Accordingly, Applicants respectfully request that the rejection of claims 9 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and the Irish Times article be reconsidered and withdrawn.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

In addition, if a new office action is deemed necessary by the Examiner in this case, Applicants respectfully request that the new office action be a non-final office action. In particular, Applicants did not receive a copy of the office action until three days immediately prior to the expiration of the extended period for reply. According to the Examiner, the office action was returned to the Office undelivered, and despite Applicants efforts to have the address of record changed, the Office neglected to send the office action to the proper address. Because of the failure of the Office to resend the office action to the correct address, Applicants did not have sufficient time to fully prepare a response. Therefore, Applicants submit that the next office action, if necessary, should be a non-final office action to give the Applicants a fair opportunity to reply.

Furthermore, Applicants believe that a new non-final office action is appropriate because the Examiner's rejections did not accurately reflect the language of the currently pending claims.

In particular, the rejection of claim 1, in particular, asserted that Wright discloses "transforming the encrypted document with a proxy key to create a transformed document, wherein the encrypted document remains in an encrypted state during the transformation to the tranformed document" instead of the claimed limitation "applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation."

In addition, the rejection of claim 13, in particular, asserted that Wright discloses "a transformation system that transforms the encrypted document with a proxy key to create a transformed document, wherein the encrypted document remains in an encrypted state during the transformation to the tranformed document" instead of the claimed limitation "a transformation system that applies the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation."

Therefore, Applicants believe they are entitled to a new non-final office action that accurately reflects the language of the currently pending claims to ensure that the Examiner is fully considering the subject matter of the claimed invention.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: April 30, 2007

/Stephen M. Hertzler, Reg. # 58,247/
Stephen M. Hertzler

Customer No.: 22204
NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000